

ON THE DEGREE OF A KLOOSTERMAN SUM AS AN ALGEBRAIC INTEGER

KEIJO KONONEN, MARKO RINTA-AHO, AND KEIJO VÄÄNÄNEN

ABSTRACT. The maximal degree over rational numbers that an n -dimensional Kloosterman sum defined over a finite field of characteristic p can achieve is known to be $\frac{p-1}{d}$ where $d = \gcd(p-1, n+1)$. Wan has shown that this maximal degree is always achieved in points whose absolute trace is nonzero. By the works of Fischer, Wan we know that there exist many finite fields for which the values of the Kloosterman sums are distinct except Frobenius conjugation. For these fields we completely determine the degrees of all the Kloosterman sums. Even if the finite field does not satisfy this condition we can still often find points in which the Kloosterman sum has smaller degree than $\frac{p-1}{d}$.

1. INTRODUCTION

Let p, q, r be positive integers, p a prime and $q = p^r$. We denote by \mathbb{F}_q the finite field of q elements and by Tr the absolute trace function $\mathbb{F}_q \rightarrow \mathbb{F}_p$. Also, let $\zeta_p := e^{2\pi i/p}$ be a complex primitive p th root of unity. The n -dimensional Kloosterman sum at a point $a \in \mathbb{F}_q$ is defined by the equation

$$\text{Kl}_n(q, a) = \sum_{x_1, x_2, \dots, x_n \in \mathbb{F}_q^*} \psi \left(x_1 + x_2 + \dots + x_n + \frac{a}{x_1 x_2 \dots x_n} \right),$$

where $\psi : \mathbb{F}_q \rightarrow \mathbb{Q}(\zeta_p)$ is the canonical additive character of the field \mathbb{F}_q defined by $\psi(x) = \zeta_p^{\text{Tr}(x)}$.

Obviously the values of the Kloosterman sums are algebraic integers of the cyclotomic field $\mathbb{Q}(\zeta_p)$. For every index $i \in \mathbb{F}_p^*$ we let σ_i denote the unique \mathbb{Q} -automorphism of the field $\mathbb{Q}(\zeta_p)$ mapping ζ_p to ζ_p^i . The mapping $i \mapsto \sigma_i$ is an isomorphism between the multiplicative group \mathbb{F}_p^* of the prime field \mathbb{F}_p and the Galois group $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ of the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Since \mathbb{F}_p^* is cyclic there exists a unique subgroup of order d for every positive factor d of $p-1$. It follows by the main theorem of the Galois theory that there exists a unique intermediate field (denoted by E_d from now on) of degree $\frac{p-1}{d}$ over \mathbb{Q} between \mathbb{Q} and $\mathbb{Q}(\zeta_p)$. This is the fixed field of the order d subgroup. Since this is a cyclic group, $x \in E_d$ if and only if $\sigma_i(x) = x$ for some (and hence for all) $i \in \mathbb{F}_p^*$ of order d .

Key words and phrases. cyclotomic field, Kloosterman sum.

A simple calculation shows that $\sigma_i(\text{Kl}_n(q, a)) = \text{Kl}_n(q, i^{n+1}a)$ for all $i \in \mathbb{F}_p^*$. Put $d := \gcd(n+1, p-1)$ and let i_d be a generator for the unique subgroup of order d of \mathbb{F}_p^* . Then $\sigma_{i_d}(\text{Kl}_n(q, a)) = \text{Kl}_n(q, i_d^{n+1}a) = \text{Kl}_n(q, a)$ so that $\text{Kl}_n(q, a) \in E_d$ for all $a \in \mathbb{F}_q$. On the converse direction we have the following result by Wan [Wan95].

Theorem 1. *Let $a \in \mathbb{F}_q^*$ be such that $\text{Tr}(a) \neq 0$. Then $\text{Kl}_n(q, a)$ generates the unique intermediate field between \mathbb{Q} and $\mathbb{Q}(\zeta_p)$ of degree $\frac{p-1}{d}$ over \mathbb{Q} .*

In the present work our aim is to further characterize the field generated by $\text{Kl}_n(q, a)$ also in the case $\text{Tr}(a) = 0$. This is possible by using a method we already briefly outlined in [KRäV10]. We consider when $\sigma_i(\text{Kl}_n(q, a)) = \text{Kl}_n(q, a)$, ie. when

$$(1) \quad \text{Kl}_n(q, i^{n+1}a) = \text{Kl}_n(q, a).$$

Since the Kloosterman sum is invariant under Frobenius conjugation, ie. $\text{Kl}_n(q, a^{p^s}) = \text{Kl}_n(q, a)$, (1) is true if there exists some $s \in \{0, 1, \dots, r-1\}$ such that

$$(2) \quad i^{n+1}a = a^{p^s}.$$

Furthermore there exist some fields for which the values of Kloosterman sums are distinct except Frobenius conjugation ie. that satisfy

$$(3) \quad \text{Kl}_n(q, a) = \text{Kl}_n(q, b) \implies b = a^{p^s} \text{ for some } s \in \{0, 1, \dots, r-1\}.$$

For these fields (1) holds if and only if (2) is true for some s and we obtain the following theorem which completely characterizes the field generated by $\text{Kl}_n(q, a)$.

Theorem 2. *Assume that the field \mathbb{F}_q satisfies (3) and denote $R := \gcd(\frac{p-1}{d}, r)$. Also, let γ be a primitive element for \mathbb{F}_q . Then each Kloosterman sum $\text{Kl}_n(q, a)$ for $a \in \mathbb{F}_q^*$ generates some intermediate field between E_{dR} and E_d . For $e|R$, $e > 1$ we have $\text{Kl}_n(q, a) \in E_{de}$ if and only if there exists a positive divisor t of $\frac{r}{e}$ and $u \in \{1, \dots, e-1\}$ satisfying $\gcd(e, u) = 1$ such that $a \in \sqrt[e]{\gamma_t^u} \mathbb{F}_{p^t}^*$ where*

$$\sqrt[e]{\gamma_t} := \gamma^{\frac{p^r-1}{e(p^t-1)}}$$

is an e th root of the primitive element γ_t of \mathbb{F}_{p^t} .

Fischer [Fis92] has shown that (3) holds for all fields satisfying the bound $p > (2(n+1)^{2r} + 1)^2$. The referee of the Fischer's paper conjectured that the much stricter bound $p \geq r(n+1)$ should actually hold. Further remarkable progress on this question has been made by Wan in the previously mentioned work [Wan95]. Among other things Wan showed that (3) holds with the bound $p \geq (r-1)(n+1) + 2$ provided the prime p does not divide any of the terms in a certain rather complicated finite sequence. Especially it follows from Wan's results that

referee's conjecture holds in the case of classical Kloosterman sums ($n = 1$) for many small values of r except possibly some small number of exceptional values of p . In particular, it holds for all p in the case $n = 1, r \leq 4$.

Even if the field \mathbb{F}_q does not satisfy (3) we still have the next partial result.

Theorem 3. *Let $e \mid \gcd(\frac{p-1}{d}, r)$, $e > 1$. We have $\text{Kl}_n(q, a) \in E_{de}$ if there exists a positive divisor t of $\frac{r}{e}$ and $u \in \{1, \dots, e-1\}$ satisfying $\gcd(e, u) = 1$ such that $a \in \sqrt[e]{\gamma_t^u} \mathbb{F}_{p^t}^*$ (using the same notation as in Theorem 2).*

2. THE PROOF OF THEOREMS 2 AND 3

We need the following elementary fact.

Lemma 4. *Let $m \mid n$. Then $x + n\mathbb{Z} \mapsto x + m\mathbb{Z}$ defines a surjective homomorphism $(\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathbb{Z}/m\mathbb{Z})^*$.*

Proof. Write $n = MQ$ where $\gcd(Q, m) = 1$ and M is the product of all prime factors l of n such that $l \mid m$ (counting multiplicities). Let $y + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^*$. We shall show that at least one of $y, y + m, \dots, y + (Q-1)m$ is relatively prime to n .

Put $k_i := \gcd(n, y + im)$ for every $i \in \mathbb{Z}$. We have $\gcd(m, y + im) = \gcd(m, y) = 1$ and therefore also $\gcd(M, y + im) = 1$. It follows that $k_i = \gcd(Q, y + im)$ for every i . Notice that the elements $(y + im) + Q\mathbb{Z}$ for $i = 0, 1, \dots, Q-1$ form a coset of the additive subgroup of $\mathbb{Z}/Q\mathbb{Z}$ generated by m . Since $\gcd(m, Q) = 1$ this subgroup is actually whole $\mathbb{Z}/Q\mathbb{Z}$. Consequently, there exists an $i \in \{0, 1, \dots, Q-1\}$ such that $k_i = \gcd(Q, y + im) = 1$. \square

Denote $\gamma_t = \gamma^{(p^r-1)/(p^t-1)}$ whenever $t \mid r$ so that γ_t is a primitive element for \mathbb{F}_{p^t} . Assume that $e \mid \frac{p-1}{d}$ and $a \in \mathbb{F}_q^*$. Our idea is to determine when $\text{Kl}_n(q, a) \in E_{de}$. Obviously this is the case if and only if (1) holds for a generator i of the order ed subgroup of \mathbb{F}_p^* . We shall use $i = \gamma_1^{(p-1)/ed}$. Obviously (1) is satisfied if there exists an $s \in \{0, 1, \dots, r-1\}$ such that (2) holds. Moreover, if we assume (3) (that is in the case of Theorem 2) we find that (1) is satisfied if and only if there exists an $s \in \{0, 1, \dots, r-1\}$ such that (2) holds.

Let us now try to find out all a and s such that (2) is satisfied for a fixed e . For $s = 0$ and any $a \in \mathbb{F}_q^*$ we see that (2) is true if and only if $i^{n+1} = 1$. This corresponds to the trivial case $e = 1$. From now on we shall assume $e > 1$ and $s > 0$. Put $a = \gamma^x$. Then (2) is equivalent to

$$(4) \quad (p^s - 1)x \equiv \frac{n+1}{d} \frac{p^r - 1}{e} \pmod{p^r - 1}.$$

Note that $\gcd(\frac{n+1}{d}, \frac{p-1}{d}) = 1$ by definition of d and therefore also $\gcd(e, \frac{n+1}{d}) = 1$.

We have $\gcd(p^s - 1, p^r - 1) = p^t - 1$ where $t := t_s := \gcd(r, s)$. Put $r = r't$ and $s = s't$. Now (4) is solvable if and only if $(p^t - 1) \mid \frac{n+1}{d} \frac{p^r - 1}{e}$ ie. if and only if $e \mid \frac{n+1}{d} \frac{p^r - 1}{p^t - 1}$. Because $\gcd(e, \frac{n+1}{d}) = 1$ this is equivalent to $e \mid \gcd(\frac{p-1}{d}, \frac{p^r - 1}{p^t - 1})$. Notice that

$$\frac{p^r - 1}{p^t - 1} = (p^t - 1)(p^{t(r'-2)} + 2p^{t(r'-3)} + \dots + (r' - 2)p^t + (r' - 1)) + r'.$$

Since $\frac{p-1}{d} \mid (p^t - 1)$ we must have $\gcd(\frac{p-1}{d}, \frac{p^r - 1}{p^t - 1}) = \gcd(\frac{p-1}{d}, r')$. Thus, for a fixed e and s satisfying $\gcd(r, s) = t$, (4) is solvable if and only if $e \mid \gcd(\frac{p-1}{d}, \frac{r}{t})$.

Let us now assume that (4) is solvable for a given s and let us find all solutions a for this s . The congruence (4) will then be equivalent to

$$(5) \quad \frac{p^s - 1}{p^t - 1} x \equiv \frac{n+1}{d} \frac{p^r - 1}{e(p^t - 1)} \pmod{\frac{p^r - 1}{p^t - 1}}.$$

Denote $C_{s,t} := \frac{p^s - 1}{p^t - 1}$ for all s, t . Assume that $C_{s,t} C_{s,t}^* \equiv 1 \pmod{C_{r,t}}$. Then we can write the solutions for (5) in the form $x \equiv \frac{n+1}{d} C_{s,t}^* \frac{C_{r,t}}{e} \pmod{C_{r,t}}$. We have $p \equiv 1 \pmod{e}$ and therefore also

$$C_{s,t} = \frac{p^{ts'} - 1}{p^t - 1} = p^{t(s'-1)} + \dots + p^t + 1 \equiv s' \pmod{e}.$$

Using this information the solution for (5) comes

$$x \equiv \frac{n+1}{d} \frac{s^* C_{r,t}}{e} \pmod{C_{r,t}}$$

where s^* is such that $s's^* \equiv 1 \pmod{e}$.

Notice that if (4) is solvable for some s then it will also be solvable (with the same e) for all other s satisfying $\gcd(r, s) = t$. There are $\varphi(\frac{r}{t})$ such values of s , namely $s = s't$, where $1 \leq s' < \frac{r}{t}$ and $\gcd(s', r') = 1$. Since $e \mid \frac{r}{t}$ it follows from Lemma 4 that $s' \pmod{e}$ and consequently also $s^* \frac{n+1}{e}$ will run through the reduced residue system modulo e (possibly several times) when s goes through all the above values. Thus all the solutions x for all s giving rise to fixed $t \mid r$ and for this fixed e will be

$$x = u \frac{p^r - 1}{e(p^t - 1)} + v \frac{p^r - 1}{p^t - 1}$$

where $u \in \{1, 2, \dots, e-1\}$, $\gcd(e, u) = 1$ and $v \in \{0, 1, \dots, p^t - 2\}$. Obviously we can write these solutions in the claimed form $a = \gamma^x \in \sqrt[e]{\gamma_t^u} \mathbb{F}_{p^t}^*$.

From the preceeding discussion it follows that there exists t such that (4) is solvable for the corresponding s if and only if $e \mid R$. In particular, under the assumption (3) this means that $\text{Kl}_n(q, a)$ generates some intermediate field of E_{dR} and E_d for all $a \in \mathbb{F}_q^*$. Furthermore, if solutions exist then the set of all t for which (4) is solvable consists positive divisors $t \mid \frac{r}{e}$ (assuming $e > 1$). Gathering all the information together we have the claimed results.

3. FURTHER OBSERVATIONS

We note that in Theorems 2 and 3 the condition denoted by (i) below can be written in the equivalent form (ii).

- (i) $a \in \sqrt[e]{\gamma_t^u} \mathbb{F}_{p^t}^*$, for some $u \in \{0, 1, \dots, e-1\}$ relatively prime to e .
- (ii) $k = e$ is the smallest positive exponent such that $a^k \in \mathbb{F}_{p^t}^*$.

It follows from the Wan's result (Theorem 1) that $\text{Tr}(a) = 0$ whenever $\text{Kl}_n(q, a) \in E_{de}$ for $e > 1$. We can, however, also see this directly for the values of a obtained from the preceding theorems. Assume $e > 1$, $e \mid \gcd(\frac{p-1}{d}, r)$ and $t \mid_e^r$. Let $a \in \mathbb{F}_q^*$ be such that $k = e$ is the smallest exponent for which $a^k \in \mathbb{F}_{p^t}$. We have already seen in the previous section that $p \equiv 1 \pmod{e}$ implies $\frac{p^{et}-1}{p^t-1} \equiv e \pmod{e}$. It follows that $\sqrt[e]{\gamma_t} \in \mathbb{F}_{p^{et}}$ and thus also $a \in \mathbb{F}_{p^{et}}$. We have

$$\text{Tr}_{\mathbb{F}_{p^{et}}/\mathbb{F}_{p^t}}(a) = a \left(1 + a^{p^t-1} + \dots + a^{p^{t(e-1)}-1} \right).$$

Since $a^e \in \mathbb{F}_{p^t}$ and $e \mid (p-1)$ we see that $(1 + a^{p^t-1} + \dots + a^{p^{t(e-1)}-1}) \in \mathbb{F}_{p^t}$. By the properties of the trace function also $\text{Tr}_{\mathbb{F}_{p^{et}}/\mathbb{F}_{p^t}}(a) \in \mathbb{F}_{p^t}$ and by assumptions $a \notin \mathbb{F}_{p^t}$. This is possible if and only if

$$\text{Tr}_{\mathbb{F}_{p^{et}}/\mathbb{F}_{p^t}}(a) = 0.$$

From this sharper result it follows, by using the transitivity of the trace, that $\text{Tr}(a) = 0$.

As a special case of our results we can characterize some – all in the case of (3) – points where the Kloosterman sum obtains a rational value.

Corollary 5. *Assume that $\frac{p-1}{d} \mid r$. We have $\text{Kl}_n(q, a) \in \mathbb{Q}$ if there exists a positive divisor t of $\frac{dr}{p-1}$ such that $k = \frac{p-1}{d}$ is the smallest positive exponent for which $a^k \in \mathbb{F}_{p^t}$.*

Furthermore, if \mathbb{F}_q satisfies (3) there are no other values $a \in \mathbb{F}_q^$ besides the above for which $\text{Kl}_n(q, a) \in \mathbb{Q}$. In particular, in the case $\frac{p-1}{d} \nmid r$ there exists no $a \in \mathbb{F}_q^*$ for which $\text{Kl}_n(q, a) \in \mathbb{Q}$.*

REFERENCES

- [Fis92] Benji Fisher. Distinctness of Kloosterman Sums. In *Contemporary Mathematics: p-Adic Methods in Number Theory and Algebraic Geometry*, pages 81–102. American Mathematical Society, 1992.
- [KRäV10] Keijo Kononen, Marko Rinta-aho, and Keijo Väänänen. On integer values of Kloosterman sums. *IEEE Transactions on Information Theory*, 56(8):4011–4013, 2010.
- [Wan95] Daqing Wan. Minimal Polynomials and Distinctness of Kloosterman Sums. *Finite Fields and Their Applications*, 1(2):189–203, 1995.

E-mail address: keijo.kononen@oulu.fi

E-mail address: marko.rinta-aho@oulu.fi

E-mail address: keijo.vaananen@oulu.fi

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF OULU, P.O.
BOX 3000, FIN-90014 OULUN YLIOPISTO, FINLAND